GLBP の設定

- 『Configuring GLBP』 （1 ページ）

『Configuring GLBP』

ゲートウェイ ロード バランシング プロトコル（GLBP）は、ホットスタンバイ ルータ プロトコル（HSRP）や仮想ルータ冗長プロトコル（VRRP）のように、機能を停止したデバイスや回路からデータ トラフィックを保護します。このとき、冗長化されたデバイスのグループ間でパケットのロード シェアリングを行うことができます。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、使用するプラットフォームおよびソフトウェア リリースの Bug Search Tool およびリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

GLBP の制限事項

拡張オブジェクト トラッキング（EOT）はステートフル スイッチオーバー（SSO）を認識しないため、SSO モードで GLBP と併用することはできません。

GLBP の前提条件

GLBP を設定する前に、デバイスが物理インターフェイス上の複数の MAC アドレスをサポートできることを確認してください。設定している GLBP フォワーダごとに、追加の MAC アドレスが使用されます。

GLBP に関する情報

GLBP の概要

GLBP は、IEEE 802.3 LAN 上でデフォルト ゲートウェイを 1 つだけ指定して設定された IP ホストの自動デバイス バックアップを行います。LAN 上の複数のファーストホップ デバイスを連結し、IP パケットの転送負荷を共有しながら単一の仮想ファーストホップ IP デバイスを提供します。LAN 上にあるその他のデバイスは、冗長化された GLBP デバイスとして動作できます。このデバイスは、既存のフォワーディング デバイスが機能しなくなった場合にアクティブになります。

GLBP は、ユーザに対しては HSRP や VRRP と同様の機能を実行します。HSRP および VRRP は、仮想 IP アドレスを指定して設定された仮想デバイス グループに、複数のデバイスを参加させます。グループの仮想 IP アドレスに送信されたパケットを転送するアクティブ デバイスとして、1 つのメンバが選択されます。グループ内の他のデバイスは、アクティブ デバイスで障害が発生するまでは冗長デバイスです。これらのスタンバイ デバイスには、プロトコルによって使用されていない未使用帯域幅があります。同じデバイス セットに対して複数の仮想デバイス グループを設定できますが、ホストは異なるデフォルト ゲートウェイに対して設定する必要があります。その結果、管理上の負担が大きくなります。GLBP には、単一の仮想 IP アドレスと複数の仮想 MAC アドレスを使用して、複数のデバイス（ゲートウェイ）上でのロードバランシングを提供するというメリットがあります。転送負荷は、GLBP グループ内のすべてのデバイス間に分散されるため、単一のデバイスだけが処理して残りのデバイスがアイドルのままになるようなことはありません。各ホストは、同じ仮想 IP アドレスで設定され、仮想デバイス グループ内のすべてのデバイスが参加してパケットの転送を行います。GLBP メンバは、Hello メッセージを使用して相互に通信します。このメッセージは 3 秒ごとにマルチキャスト アドレス 224.0.0.102、UDP ポート 3222（送信元と宛先）に送信されます。

GLBP パケット タイプ

GLBP は実行に 3 つの異なるパケット タイプを使用します。そのパケット タイプは、Hello、要求、および応答です。Hello パケットはプロトコル情報をアドバタイズするために使用されます。Hello パケットはマルチキャストで、仮想ゲートウェイまたはバーチャル フォワーダが Speak、Standby、Active のいずれかの状態のときに送信されます。要求パケットと応答パケットは、仮想 MAC アドレスの割り当てに使用されます。これらはどちらもアクティブ仮想ゲートウェイ（AVG）間のユニキャスト メッセージです。

GLBP アクティブ仮想ゲートウェイ

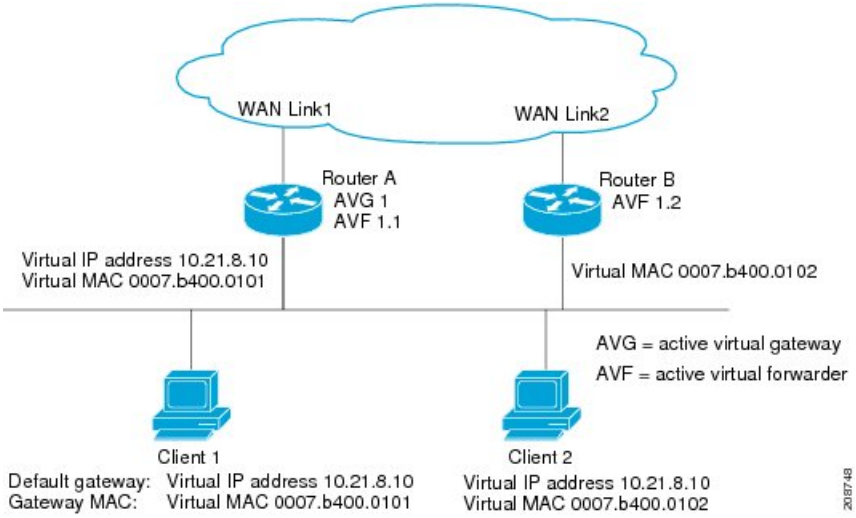
GLBP グループのメンバは、1 つのゲートウェイをそのグループのアクティブ仮想ゲートウェイ（AVG）として選択します。他のグループ メンバは、AVG が使用できなくなった場合のバックアップとなります。AVG は GLBP グループの各メンバに仮想 MAC アドレスを割り当てます。各ゲートウェイは、AVG によって割り当てられている仮想 MAC アドレスに送信されたパケットを転送する役割を引き継ぎます。これらのゲートウェイは、仮想 MAC アドレスのアクティブ仮想フォワーダ（AVF）と呼ばれます。

AVG は、仮想 IP アドレスのアドレス解決プロトコル（ARP）要求への応答も行います。ロード シェアリングは、AVG が異なる仮想 MAC で ARP 要求に応答することによって行われます。

noglbpload-balancing コマンドが設定されている場合は、AVG が AVF を備えていなければ、先頭のバーチャル フォワーダ（VF）の MAC アドレスで ARP 要求に応答します。そのため、その VF が現在の AVG に戻るまでは、トラフィックが別のゲートウェイ経由でルーティングされる可能性があります。

下の図では、ルータ A（またはデバイス A）は GLBP グループの AVG で、仮想 IP アドレス 10.21.8.10 に関する処理を行います。ルータ A は、仮想 MAC アドレス 0007.b400.0101 の AVF でもあります。ルータ B（またはデバイス B）は同じ GLBP グループのメンバであり、仮想 MAC アドレス 0007.b400.0102 の AVF として指定されています。クライアント 1 のデフォルト ゲートウェイ IP アドレスは 10.21.8.10、ゲートウェイ MAC アドレスは 0007.b400.0101 です。クライアント 2 は、同じデフォルト ゲートウェイ IP アドレスを共有しますが、ルータ B がルータ A とトラフィック負荷を分担するため、ゲートウェイ MAC アドレス 0007.b400.0102 が与えられます。

図 *1 : GLBP* トポロジ



ルータ A が使用できなくなった場合でも、クライアント 1 は WAN にアクセスできます。これは、ルータ B がルータ A の仮想 MAC アドレスに送信されたパケットの転送を引き継ぎ、ルータ B 自身の仮想 MAC アドレスに送信されたパケットに応答するからです。ルータ B は、GLBP グループ全体の AVG の役割も引き継ぎます。GLBP グループ内のデバイスで障害が発生しても、GLBP メンバの通信は継続されます。

GLBP 仮想 MAC アドレスの割り当て

GLBP グループごとに最大 4 つの仮想 MAC アドレスを設定できます。AVG は、仮想 MAC アドレスをグループの各メンバに割り当てます。他のグループ メンバは、hello メッセージを通じて AVG を検出したあとで仮想 MAC アドレスを要求します。ゲートウェイには、シーケンスにおける次の MAC アドレスが割り当てられます。AVG によって仮想 MAC アドレスが割り当てられた仮想フォワーダは、プライマリ仮想フォワーダと呼ばれます。GLBP グループの他

のメンバは、hello メッセージから仮想 MAC アドレスを学習します。仮想 MAC アドレスを学習した仮想フォワーダは、セカンダリ仮想フォワーダと呼ばれます。

GLBP 仮想ゲートウェイの冗長性

GLBP では、HSRP と同じ方法で仮想ゲートウェイの冗長性が実現されます。1 つのゲートウェイが AVG として選択され、もう 1 つのゲートウェイがスタンバイ仮想ゲートウェイとして選択されます。残りのゲートウェイはリッスン状態になります。

AVG の機能が停止すると、スタンバイ仮想ゲートウェイが該当する仮想 IP アドレスの処理を担当します。その後、リッスン状態のゲートウェイから新しいスタンバイ仮想ゲートウェイが選択されます。

GLBP 仮想フォワーダの冗長性

仮想フォワーダの冗長化は、AVF で使用する仮想ゲートウェイの冗長化に類似しています。AVF で障害が発生すると、リッスン状態のセカンダリ仮想フォワーダの 1 つが仮想 MAC アドレスの役割を引き継ぎます。

新しい AVF は、別のフォワーダ番号のプライマリ仮想フォワーダでもあります。GLBP は、ゲートウェイがアクティブ仮想フォワーダ状態に変わるとすぐに始動する 2 つのタイマーを使用して、古いフォワーダ番号からホストを移行します。GLBP は hello メッセージを使用してタイマーの現在の状態を通信します。

リダイレクト時間は、AVG がホストを古い仮想フォワーダ MAC アドレスにリダイレクトし続ける時間です。リダイレクト時間が経過すると、仮想フォワーダが、古い仮想フォワーダ MAC アドレスに送信されたパケットを転送し続けても、AVG は、ARP 応答で古い仮想フォワーダ MAC アドレスの使用を停止します。

仮想フォワーダが有効である時間は、セカンダリ ホールド時間になります。セカンダリ ホールド時間が経過すると、GLBP グループのすべてのゲートウェイから仮想フォワーダが削除されます。期限切れになった仮想フォワーダ番号は、AVG による再割り当てが可能になります。

GLBP ゲートウェイのプライオリティ

各 GLBP ゲートウェイが果たすロールと、AVG の機能が停止したときにどのようなことが発生するかについては、GLBP ゲートウェイ プライオリティによって決まります。

また、GLBP デバイスがバックアップ仮想ゲートウェイとして機能するかどうか、および現在の AVG で障害が発生した場合に AVG になる順番も決まります。各バックアップ仮想ゲートウェイのプライオリティには、**glbppriority** コマンドを使用して 1 ～ 255 の値を設定できます。

「GLBP トポロジ」の図では、LAN トポロジ内の AVG であるルータ A（またはデバイス A）で障害が発生すると、選択プロセスが実行され、処理を引き継ぐバックアップ仮想ゲートウェイが決定されます。この例では、ルータ B（またはデバイス B）がグループ内の唯一の他のメンバであるため、ルータ B（またはデバイス B）が自動的に新しい AVG になります。同じ GLBP グループ内にプライオリティの高い別のデバイスが存在していた場合は、そのプライオリティの高いデバイスが選択されます。両方のデバイスのプライオリティが同じである場合

は、IP アドレスが大きい方のバックアップ仮想ゲートウェイが選択され、アクティブ仮想ゲートウェイになります。

デフォルトでは、GLBP 仮想ゲートウェイのプリエンプティブ方式はディセーブルになっています。バックアップ仮想ゲートウェイが AVG になるのは、仮想ゲートウェイに割り当てられているプライオリティにかかわらず、現在の AVG で障害が発生した場合だけです。**glbppreempt** コマンドを使用すると、GLBP 仮想ゲートウェイのプリエンプティブ方式をイネーブルにすることができます。プリエンプションを使用すると、バックアップ仮想ゲートウェイに現在の AVG よりも高いプライオリティが割り当てられている場合に、そのバックアップ仮想ゲートウェイを AVG にすることができます。

GLBP ゲートウェイの重み付けとトラッキング

GLBP では、重み付けによって GLBP グループ内の各デバイスの転送容量を決定します。GLBP グループ内のデバイスに割り当てられた重み付けを使用して、そのルータがパケットを転送するかどうか、転送する場合はパケットを転送する LAN 内のホストの比率を決定できます。しきい値は、GLBP の重み付けが一定の値を下回ったときに転送を無効化し、別のしきい値を上回ったときには自動的に転送を再度有効化にするように設定できます。

GLBP グループの重み付けは、デバイス内のインターフェイス状態のトラッキングによって自動的に調整できます。追跡対象のインターフェイスがダウンした場合、GLBP グループの重み付けは指定された値だけ小さくなります。GLBP の重み付けの減少値は、追跡対象のインターフェイスごとに変えることができます。

デフォルトでは、GLBP 仮想フォワーダのプリエンプティブ方式はイネーブルになっており、遅延は 30 秒です。現在の AVF の重み付けが下限しきい値を下回り、その状態で 30 秒経過すると、バックアップ仮想フォワーダが AVF になります。**noglbpforwarderpreempt** コマンドを使用して GLBP 転送のプリエンプティブ方式を無効化するか、**glbpforwarderpreemptdelayminimum** コマンドを使用して遅延を変更することができます。

GLBP MD5 認証

GLBP MD5 認証は、信頼性とセキュリティを向上させるために業界標準の MD5 アルゴリズムを採用しています。MD5 認証を使用すると、別のプレーン テキスト認証方式よりもセキュリティを強化でき、スプーフィング ソフトウェアから保護できます。

MD5 認証では、各 GLBP グループ メンバが秘密キーを使用して、発信パケットに含まれるキー付き MD5 ハッシュを生成できます。着信パケットのキー付きハッシュが生成され、着信パケット内のハッシュが生成されたハッシュに一致しない場合、そのパケットは無視されます。

MD5 ハッシュのキーは、キーストリングを使用して設定で直接指定するか、またはキーチェーンを使用して間接的に指定できます。キーストリングは、100 文字の長さを超えることはできません。

デバイスは、GLBP グループに対する認証設定と異なる設定を持つデバイスからの着信 GLBP パケットを無視します。GLBP には、次の 3 つの認証方式があります。

- 認証なし
- プレーン テキスト認証

- MD5 認証

GLBP パケットは、次のいずれかの場合に拒否されます。

- 認証方式がデバイスと着信パケットの間で異なっている。
- MD5 ダイジェストがデバイスと着信パケットで異なる。
- テキスト認証文字列がデバイスと着信パケットで異なる。

ISSU-GLBP

GLBP はインサービス ソフトウェア アップグレード（ISSU）をサポートします。ISSU を使用すると、アクティブおよびスタンバイのルート プロセッサ（RP）またはライン カード上で異なるバージョンの Cisco IOS ソフトウェアが実行されている場合でも、ハイアベイラビリティ（HA）システムをステートフル スイッチオーバー（SSO）モードで実行できるようになります。

ISSU は、サポートされる Cisco IOS Release から別のリリースへアップグレードまたはダウングレードする機能を提供します。この場合、パケット転送は継続して行われ、セッションは維持されるため、予定されるシステムの停止時間を短くすることができます。アップグレードまたはダウングレードする機能は、アクティブ RP およびスタンバイ RP 上で異なるバージョンのソフトウェアを実行することで実現します。これにより、RP 間でステート情報を維持する時間が短くなります。この機能により、システムをアップグレード対象（またはダウングレード対象）のソフトウェアを実行するセカンダリ RP に切り替えることができ、セッションを切断することなく、またパケットの損失も最小限に抑えながら、継続してパケットを転送できます。この機能は、デフォルトでイネーブルにされています。

GLBP SSO

GLBP SSO 機能が導入されたため、GLBP はステートフル スイッチオーバー（SSO）を認識するようになりました。GLBP は、デバイスがセカンダリ ルータ プロセッサ（RP）にフェールオーバーしたことを検出し、グループの現在の状態を継続することができます。

SSO は、デュアル RP をサポートするネットワーキング デバイス（通常はエッジ デバイス）で機能します。1 台の RP をアクティブ プロセッサとして設定し、他の RP をスタンバイ プロセッサとして設定することで、RP 冗長化を実現します。また、RP 間の重要なステート情報を同期するため、ネットワーク ステート情報は RP 間でダイナミックに維持されます。

SSO を認識せずに RP が冗長化されたデバイスに GLBP を展開した場合、アクティブ RP とスタンバイ RP 間のロールがスイッチオーバーされると、デバイスの GLBP グループ メンバとしてのアクティビティは破棄され、デバイスはリロードされた場合と同様にグループに再び参加することになります。GLBP SSO 機能により、スイッチオーバーが行われても、GLBP は継続してグループ メンバとしてのアクティビティを継続できます。冗長化された RP 間の GLBP ステート情報は維持されるため、スタンバイ RP はスイッチオーバーの実行中も実行後も GLBP 内で引き続きデバイスのアクティビティを実行できます。

この機能は、デフォルトでイネーブルにされています。この機能をディセーブルにするには、グローバル コンフィギュレーション モードで **noglbpsso** コマンドを使用します。

GLBP の利点

ロード シェアリング

LAN クライアントからのトラフィックを複数のデバイスで共有するように GLBP を設定できるため、利用可能なデバイス間でより公平にトラフィックの負荷を共有できます。

複数の仮想デバイス

GLBP では、デバイスの各物理インターフェイス上に最大 1024 台の仮想デバイス（GLBP グループ）とグループごとに最大 4 つの仮想フォワーダがサポートされます。

プリエンプション

GLBP の冗長性スキームにより、使用可能になっているプライオリティの高いバックアップ仮想ゲートウェイをアクティブ仮想ゲートウェイ（AVG）にすることができます。フォワーダ プリエンプションも同じように機能しますが、フォワーダ プリエンプションはプライオリティの代わりに重み付けを使用し、デフォルトでイネーブルになっている点が異なります。

認証

GLBP は、信頼性やセキュリティを向上させて GLBP スプーフィング ソフトウェアからの保護を強化するための業界標準のメッセージ ダイジェスト 5（MD5）アルゴリズムをサポートしています。GLBP グループ内のデバイスの認証文字列が他のデバイスとは異なる場合、そのデバイスは他のグループ メンバによって無視されます。GLBP グループ メンバ間で簡単なテキスト パスワード認証方式を使用して、設定エラーを検出することもできます。

GLBP の設定方法

GLBP のカスタマイズ

GLBP 動作のカスタマイズは任意です。GLBP グループをイネーブルにすると、そのグループはすぐに動作します。GLBP グループをイネーブルにしてから GLBP をカスタマイズすると、機能のカスタマイズを完了する前にデバイスがグループの制御を引き継ぎ、AVG になる可能性があります。したがって、GLBP をカスタマイズする場合は、GLBP をイネーブルにする前に行うことを推奨します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *type number* 例： `Device(config)# interface GigabitEthernet 1/0/1`	インターフェイスのタイプおよび番号を指定し、インターフェイスコンフィギュレーションモードを開始します。
ステップ 4	**ipaddress** *ip-address mask* [**secondary**] 例： `Device(config-if)# ip address 10.21.8.32 255.255.255.0`	インターフェイスのプライマリ IP アドレスまたはセカンダリ IP アドレスを指定します。
ステップ 5	**glbp** *group***timers** [**msec**] *hellotime* [**msec**] *holdtime* 例： `Device(config-if)# glbp 10 timers 5 18`	GLBP グループ内の AVG によって連続的に送信される hello パケットの間隔を設定します。 • *holdtime* 引数には、hello パケット内の仮想ゲートウェイと仮想フォワーダの情報が無効と見なされるまでの時間を秒数で指定します。 • オプションの **msec** キーワードは、そのあとに続く引数がデフォルトの秒単位ではなくミリ秒単位であることを指定します。
ステップ 6	**glbp** *group***timersredirect** *redirect timeout* 例： `Device(config-if)# glbp 10 timers redirect 1800 28800`	AVG がクライアントを AVF にリダイレクトし続ける時間を設定します。デフォルトは 600 秒（10 分）です。 • *timeout* 引数には、セカンダリ仮想フォワーダが無効になるまでの時間を秒数で指定します。デフォルトは 14,400 秒（4 時間）です。

	コマンドまたはアクション	目的
		（注） *redirect* 引数のゼロ（0）値は、指定できる値の範囲から除外することはできません。Cisco IOS ソフトウェアの事前設定でゼロ（0）値を使用しているため、アップグレードに悪影響を及ぼすことになります。ただし、ゼロ（0）値に設定することは推奨しません。この値を使用すると、リダイレクトタイマーが期限切れになりません。リダイレクトタイマーが期限切れにならず、デバイスに障害が発生すると、新しいホストがバックアップへリダイレクトされずに、障害が発生したデバイスに引き続き割り当てられます。
ステップ 7	**glbp** *group* **load-balancing** [**host-dependent** | **round-robin** | **weighted**] 例： `Device(config-if)# glbp 10 load-balancing host-dependent`	GLBP AVG で使用するロードバランシングの方式を指定します。
ステップ 8	**glbp** *group* **priority** *level* 例： `Device(config-if)# glbp 10 priority 254`	GLBP グループ内のゲートウェイのプライオリティ レベルを設定します。 • デフォルト値は 100 です。
ステップ 9	**glbp** *group* **preempt** [**delay minimum** *seconds*] 例： `Device(config-if)# glbp 10 preempt delay minimum 60`	デバイスのプライオリティが現在の AVG よりも高い場合に、GLBP グループの AVG として処理を引き継ぐようにルータを設定します。 • このコマンドは、デフォルトでディセーブルになっています。 • AVG の交替が行われるまでの最小遅延インターバルを秒数で指定するには、オプションの **delay** キーワードおよび **minimum** キーワー

	コマンドまたはアクション	目的
		ドおよび *seconds* 引数を指定します。
ステップ 10	**glbp** *group* **client-cachemaximum** *number* [**timeout** *minutes*] 例： `Device(config-if)# glbp 10 client-cache maximum 1200 timeout 245`	（任意）GLBP クライアント キャッシュをイネーブルにします。 • このコマンドは、デフォルトでディセーブルになっています。 • *number* 引数を使用して、キャッシュがこの GLBP グループのためにホールドするクライアントの最大数を指定します。範囲は 8 ～ 2000 です。 • オプションの **timeout** *minutes* キーワードと引数のペアを使用して、クライアント情報が最後に更新されてから、クライアントエントリが GLBP クライアント キャッシュに保管される最大時間を設定します。範囲は、1 ～ 1440 分（1 日）です。 （注） IPv4 ネットワークには、予測されるエンド ホストの Address Resolution Protocol（ARP）キャッシュの最大タイムアウト値よりも若干長い GLBP クライアント キャッシュのタイムアウト値を設定することを推奨します。
ステップ 11	**glbp** *group* **name** *redundancy-name* 例： `Device(config-if)# glbp 10 name abc123`	GLBP グループに名前を割り当てることによって、IP 冗長性をイネーブルにします。 • 冗長クライアントと GLBP グループを接続できるように、GLBP 冗長クライアントに同じ GLBP グループ名を設定する必要があります。
ステップ 12	**exit** 例：	インターフェイス コンフィギュレーションモードを終了し、デバイスをグ

	コマンドまたはアクション	目的
	`Device(config-if)# exit`	ローバル コンフィギュレーション モードに戻します。
ステップ 13	**noglbpsso** 例： `Device(config)# no glbp sso`	（任意）SSO の GLBP サポートをディセーブルにします。

キー ストリングを使用した GLBP MD5 認証の設定

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *type number* 例： `Device(config)# interface GigabitEthernet 1/0/1`	インターフェイス タイプを設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**ipaddress** *ip-address mask* [**secondary**] 例： `Device(config-if)# ip address 10.0.0.1 255.255.255.0`	インターフェイスのプライマリ IP アドレスまたはセカンダリ IP アドレスを指定します。
ステップ 5	**glbp** *group-number* **authenticationmd5key-string** [**0** | **7**] *key* 例： `Device(config-if)# glbp 1 authentication md5 key-string d00b4r987654321a`	GLBP MD5 認証の認証キーを設定します。 • キー ストリングは、100 文字の長さを超えることはできません。 • *key* 引数にはプレフィックスを指定しません。**0** を指定すると、キーは暗号化されていないことを示します。

	コマンドまたはアクション	目的
		• **7** を指定すると、キーは暗号化されます。**servicepassword-encryption** グローバル コンフィギュレーション コマンドがイネーブルになっている場合、key-string 認証キーは自動的に暗号化されます。
ステップ 6	**glbp** *group-number* **ip** [*ip-address* [**secondary**]] 例： `Device(config-if)# glbp 1 ip 10.0.0.10`	インターフェイス上でGLBPを設定し、仮想ゲートウェイのプライマリ IP アドレスを指定します。
ステップ 7	通信する各デバイスに対してステップ 1 ～ 6 を繰り返します。	—
ステップ 8	**end** 例： `Device(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 9	**showglbp** 例： `Device# show glbp`	（任意）GLBP の情報を表示します。 • このコマンドを使用して、設定を確認します。設定されている場合はキー ストリングと認証タイプが表示されます。

キー チェーンを使用した GLBP MD5 認証の設定

キーチェーンを使用したGLBPMD5認証を設定するには、次の作業を実行します。キーチェーンを使用すると、キー チェーン設定に従って異なる時点で異なるキー ストリングを使用できます。GLBP は、適切なキー チェーンを照会して、指定されたキー チェーンの現在アクティブなキーとキー ID を取得します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**keychain** *name-of-chain* 例： `Device(config)# key chain glbp2`	ルーティング プロトコルの認証をイネーブルにし、認証キーのグループを識別し、キー チェーン キー コンフィギュレーション モードを開始します。
ステップ 4	**key** *key-id* 例： `Device(config-keychain)# key 100`	キー チェーンの認証キーを識別します。 • *key-id* 引数の値には数値を指定する必要があります。
ステップ 5	**key-string** *string* 例： `Device(config-keychain-key)# key-string abc123`	キーの認証文字列を指定し、キー チェーン キー コンフィギュレーション モードを開始します。 • *string* 引数の値は、1 ～ 80 文字の大文字または小文字の英数字を指定できます。最初の文字には数字を使用できません。
ステップ 6	**exit** 例： `Device(config-keychain-key)# exit`	キー チェーン キー コンフィギュレーション モードに戻ります。
ステップ 7	**exit** 例： `Device(config-keychain)# exit`	グローバル コンフィギュレーション モードに戻ります。
ステップ 8	**interface** *type number* 例： `Device(config)# interface GigabitEthernet 1/0/1`	インターフェイスタイプを設定し、インターフェイスコンフィギュレーション モードを開始します。
ステップ 9	**ipaddress** *ip-address mask* [**secondary**] 例： `Device(config-if)# ip address 10.21.0.1 255.255.255.0`	インターフェイスのプライマリ IP アドレスまたはセカンダリ IP アドレスを指定します。

	コマンドまたはアクション	目的
ステップ 10	**glbp** *group-number* **authentication md5 key-chain** *name-of-chain* 例： `Device(config-if)# glbp 1 authentication md5 key-chain glbp2`	GLBP MD5 認証の認証 MD5 キーチェーンを設定します。 • キーチェーン名は、ステップ 3 で指定した名前に一致する必要があります。
ステップ 11	**glbp** *group-number* **ip** [*ip-address* [**secondary**]] 例： `Device(config-if)# glbp 1 ip 10.21.0.12`	インターフェイス上で GLBP を設定し、仮想ゲートウェイのプライマリ IP アドレスを指定します。
ステップ 12	通信する各デバイスに対してステップ 1 ～ 10 を繰り返します。	—
ステップ 13	**end** 例： `Device(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 14	**showglbp** 例： `Device# show glbp`	（任意）GLBP の情報を表示します。 • このコマンドを使用して、設定を確認します。設定されている場合はキーチェーンと認証タイプが表示されます。
ステップ 15	**showkeychain** 例： `Device# show key chain`	（任意）認証キー情報を表示します。

GLBP テキスト認証の設定

テキスト認証は最小限のセキュリティを提供します。セキュリティが必須の場合は、MD5 認証を使用してください。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例：	特権 EXEC モードをイネーブルにします。

	コマンドまたはアクション	目的
	`Device> enable`	• パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *type number* 例： `Device(config)# interface GigabitEthernet 1/0/1`	インターフェイス タイプを設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**ipaddress** *ip-address mask* [**secondary**] 例： `Device(config-if)# ip address 10.0.0.1 255.255.255.0`	インターフェイスのプライマリ IP アドレスまたはセカンダリ IP アドレスを指定します。
ステップ 5	**glbp** *group-number* **authenticationtext** *string* 例： `Device(config-if)# glbp 10 authentication text stringxyz`	グループ内の他のデバイスから受信した GLBP パケットを認証します。 • 認証を設定する場合は、GLBP グループ内のすべてのデバイスで同じ認証文字列を使用する必要があります。
ステップ 6	**glbp** *group-number* **ip** [*ip-address* [**secondary**]] 例： `Device(config-if)# glbp 1 ip 10.0.0.10`	インターフェイス上でGLBPを設定し、仮想ゲートウェイのプライマリ IP アドレスを指定します。
ステップ 7	通信する各デバイスに対してステップ 1 ～ 6 を繰り返します。	—
ステップ 8	**end** 例： `Device(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 9	**showglbp** 例： `Device# show glbp`	（任意）GLBP の情報を表示します。 • このコマンドを使用して、設定を確認します。

GLBP の重み付けの値とオブジェクト トラッキング

GLBP 重み付けにより、GLBP グループが仮想フォワーダとして動作できるかどうかが決定されます。重み付けの初期値を設定したり、オプションのしきい値を指定したりできます。インターフェイスの状態を追跡し、インターフェイスがダウンした場合に重み付けの値を減らすための減少値を設定できます。GLBP グループの重み付けが指定の値を下回ると、グループはアクティブ仮想フォワーダでなくなります。重み付けが指定の値を上回ると、グループは再びアクティブ仮想フォワーダとしてのロールを実行できるようになります。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**track** *object-number***interface** *type number* {**line-protocol** |{**ip** | **ipv6**} **routing**} 例： `Device(config)# track 2 interface GigabitEthernet 1/0/1 ip routing`	GLBP ゲートウェイの重み付けに影響する状態変化を追跡するインターフェイスを設定し、トラッキング コンフィギュレーション モードを開始します。 • このコマンドは、**glbpweightingtrack** コマンドで使用されるインターフェイスと対応するオブジェクトの数を設定します。 • **line-protocol** キーワードを指定すると、インターフェイスがアップ状態かどうかが追跡されます。**iprouting** キーワードを指定すると、インターフェイス上でIPルーティングがイネーブルであり、IP アドレスが設定されているかどうかもチェックされます。
ステップ 4	**exit** 例： `Device(config-track)# exit`	グローバル コンフィギュレーション モードに戻ります。

	コマンドまたはアクション	目的
ステップ 5	**interface** *type number* 例： `Device(config)# interface GigabitEthernet 1/0/1`	インターフェイス コンフィギュレーション モードを開始します。
ステップ 6	**glbp** *group* **weighting** *maximum* [**lower** *lower*] [**upper** *upper*] 例： `Device(config-if)# glbp 10 weighting 110 lower 95 upper 105`	GLBP ゲートウェイの重み付けの初期値、上限しきい値、および下限しきい値を指定します。
ステップ 7	**glbp** *group* **weightingtrack** *object-number* [**decrement** *value*] 例： `Device(config-if)# glbp 10 weighting track 2 decrement 5`	GLBP ゲートウェイの重み付けに影響する、追跡対象のオブジェクトを指定します。 • *value* 引数には、追跡対象のオブジェクトで障害が発生した場合に GLBP ゲートウェイの重み付けを減らす量を指定します。
ステップ 8	**glbp** *group* **forwarderpreempt** [**delayminimum** *seconds*] 例： `Device(config-if)# glbp 10 forwarder preempt delay minimum 60`	GLBP グループの現在の AVF の値が重みしきい値よりも低くなった場合に、GLBP グループの AVF としてのロールを引き継ぐデバイスを設定します。 • このコマンドは、デフォルトでイネーブルになっており、遅延は 30 秒です。 • AVF の交替が行われるまでの最小遅延インターバルを秒数で指定するには、オプションの **delay** キーワードおよび **minimum** キーワードおよび *seconds* 引数を指定します。
ステップ 9	**exit** 例： `Device(config-if)# exit`	特権 EXEC モードに戻ります。
ステップ 10	**showtrack** [*object-number* | **brief**] [**interface** [**brief**] | **iproute** [**brief**] | **resolution** | **timers**]	トラッキング情報を表示します。

	コマンドまたはアクション	目的
	例： `Device# show track 2`	

GLBP のトラブルシューティング

GLBP には、GLBP 動作に関する各種イベントに関連する診断出力を可視化する 5 つの特権 EXEC モード コマンドが導入されています。**debugconditionglbp**、**debugglbperrors**、**debugglbpevents**、**debugglbppackets**、**debugglbpterse** の各コマンドは、トラブルシューティング専用です。これはソフトウェアによって生成される出力のボリュームが、デバイスの深刻なパフォーマンスの低下を引き起こす可能性があるためです。**debugglbp** コマンドを使用した場合の影響を最小限に抑えるには、次の作業を実行します。

この手順により、コンソール ポートが文字単位のプロセッサ割り込みを行わなくなるため、**debugconditionglbp** コマンドまたは **debugglbp** コマンドを使用することでデバイスにかかる負荷が最小限に抑えられます。直接コンソールに接続できない場合は、ターミナルサーバを介してこの手順を実行できます。ただし、Telnet 接続を切断しなければならない場合は、デバッグ出力の生成でプロセッサに負荷がかかりデバイスが応答できないことに起因して、再接続できないことがあります。

始める前に

この作業では、コンソールに直接接続された GLBP を実行しているデバイスが必要です。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**nologgingconsole** 例： `Device(config)# no logging console`	コンソール端末へのすべてのロギングをディセーブルにします。 • コンソールへのロギングを再度イネーブルにするには、グローバル コンフィギュレーション モードで **loggingconsole** コマンドを使用します。

	コマンドまたはアクション	目的
ステップ 4	Telnet を使用してデバイス ポートにアクセスし、ステップ 1 と 2 を繰り返します。	再帰 Telnet セッションでグローバル コンフィギュレーション モードを開始します。これにより、出力をコンソール ポートからリダイレクトできます。
ステップ 5	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 6	**terminalmonitor** 例： `Device# terminal monitor`	仮想端末でのロギング出力をイネーブルにします。
ステップ 7	**debugconditionglbp** *interface-type interface-number group* [*forwarder*] 例： `Device# debug condition glbp GigabitEthernet 0/0/0 1`	GLBP 状態に関するデバッグ メッセージを表示します。 • 特定の **debugconditionglbp** または **debugglbp** コマンドだけを入力して、出力を特定のサブコンポーネントに分離し、プロセッサの負荷を最小限に抑えます。適切な引数とキーワードを使用して、指定したサブコンポーネント上に詳細なデバッグ情報を生成します。 • 終了したら、特定の **nodebugconditionglbp** または **nodebugglbp** コマンドを入力します。
ステップ 8	**terminalnomonitor** 例： `Device# terminal no monitor`	仮想端末でのロギングをディセーブルにします。

GLBP の設定例

例：GLBP 設定のカスタマイズ

```
Device(config)# interface GigabitEthernet 1/0/1
Device(config-if)# ip address 10.21.8.32 255.255.255.0
Device(config-if)# glbp 10 timers 5 18
```

```
Device(config-if)# glbp 10 timers redirect 1800 28800
Device(config-if)# glbp 10 load-balancing host-dependent
Device(config-if)# glbp 10 priority 254
Device(config-if)# glbp 10 preempt delay minimum 60

Device(config-if)# glbp 10 client-cache maximum 1200 timeout 245
```

例：キー ストリングを使用した GLBP MD5 認証の設定

次に、キー ストリングを使用して GLBP MD5 認証を設定する例を示します。

```
Device(config)# interface GigabitEthernet 1/0/1
Device(config-if)# ip address 10.0.0.1 255.255.255.0
Device(config-if)# glbp 2 authentication md5 key-string ThisStringIsTheSecretKey
Device(config-if)# glbp 2 ip 10.0.0.10
```

例：キー チェーンを使用した GLBP MD5 認証の設定

次に、GLBP がキー チェーン「AuthenticateGLBP」を照会して、指定されたキー チェーンの現在アクティブなキーとキー ID を取得する例を示します。

```
Device(config)# key chain AuthenticateGLBP
Device(config-keychain)# key 1
Device(config-keychain-key)# key-string ThisIsASecretKey
Device(config-keychain-key)# exit
Device(config-keychain)# exit
Device(config)# interface GigabitEthernet 1/0/1
Device(config-if)# ip address 10.0.0.1 255.255.255.0
Device(config-if)# glbp 2 authentication md5 key-chain AuthenticateGLBP
Device(config-if)# glbp 2 ip 10.0.0.10
```

例：GLBP テキスト認証の設定

```
Device(config)# interface GigabitEthernet 0/0/0
Device(config-if)# ip address 10.21.8.32 255.255.255.0
Device(config-if)# glbp 10 authentication text stringxyz
Device(config-if)# glbp 10 ip 10.21.8.10
```

例：GLBP 重み付けの設定

次に、デバイスを POS インターフェイス 5/0/0 と 6/0/0 の IP ルーティング状態を追跡するように設定し、GLBP の重み付けの初期値、上限しきい値、下限しきい値、および重み付けの減少値 10 を設定する例を示します。POS インターフェイス 5/0/0 と 6/0/0 がダウンすると、デバイスの重み付けの値が小さくなります。

```
Device(config)# track 1 interface GigabitEthernet 1/0/1 line-protocol
Device(config)# track 2 interface GigabitEthernet 1/0/3 line-protocol
Device(config)# interface TenGigabitEthernet 0/0/1
Device(config-if)# ip address 10.21.8.32 255.255.255.0
Device(config-if)# glbp 10 weighting 110 lower 95 upper 105
Device(config-if)# glbp 10 weighting track 1 decrement 10
Device(config-if)# glbp 10 weighting track 2 decrement 10
```

例：GLBP 設定のイネーブル化

次の例では、デバイスは GLBP をイネーブルにするように設定されています。GLBP グループ 10 には、仮想 IP アドレス 10.21.8.10 が指定されています。

```
Device(config)# interface GigabitEthernet 0/0/0
Device(config-if)# ip address 10.21.8.32 255.255.255.0
Device(config-if)# glbp 10 ip 10.21.8.10
```

GLBP に関する追加情報

関連資料

関連項目	マニュアル タイトル
GLBP コマンド：コマンド構文の詳細、コマンド モード、コマンド履歴、デフォルト設定、使用上のガイドライン、および例。	『Cisco IOS IP Application Services Command Reference』
インサービス ソフトウェア アップグレード（ISSU）の設定	『*Cisco IOS High Availability Configuration Guide*』の「In Service Software Upgrade Process」のモジュール
キーチェーンおよびキー管理用コマンド：コマンド構文の詳細、コマンドモード、コマンド履歴、デフォルト設定、使用に関する注意事項、および例	『*Cisco IOS IP Routing Protocol-Independent Command Reference*』
オブジェクト トラッキング	「Configuring Enhanced Object Tracking」のモジュール
『Stateful Switchover』	『*Cisco IOS High Availability Configuration Guide*』の「Stateful Switchover」のモジュール
VRRP	「Configuring VRRP」のモジュール
HSRP	「Configuring HSRP」のモジュール
GLBP の IPv6 サポート	「FHRP - GLBP Support for IPv6」のモジュール

シスコのテクニカル サポート

説明	Link
★枠で囲まれた Technical Assistance の場合★右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

GLBP の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *1 : GLBP* の機能情報

機能名	リリース	機能の設定情報
Gateway Load Balancing Protocol		GLBP は、冗長化されたルータ グループ間でパケットのロード シェアリングを行う一方、タ トラフィックを保護します。 Cisco IOS Release Cisco IOS XE Release 3.6E では、この機能は以下のプラットフォームでサ • Cisco 5760 Wireless LAN Controller 次のコマンドがこの機能によって導入、または変更されました： **glbpforwarderpreemptglbpipglbpload-balancingglbpnameglbppreemptglbppriorityglbpssoglbp**

機能名	リリース	機能の設定情報
GLBP MD5 認証	Cisco IOS XE 3.6E	MD5 認証を使用すると、別のプレーン テキスト認証方式よりもセキュリティを強化で して、発信パケットに含まれるキー付きMD5ハッシュを生成できます。着信パケットの れたハッシュに一致しない場合、そのパケットは無視されます。 Cisco IOS Release Cisco IOS XE Release 3.6E では、この機能は以下のプラットフォームで • Cisco 5760 Wireless LAN Controller **glbpauthentication** および **showglbp** の各コマンドがこの機能により変更されました。
ISSU と GLBP		GLBP はインサービス ソフトウェア アップグレード（ISSU）をサポートします。ISSU （RP）またはライン カード上で異なるバージョンの Cisco IOS ソフトウェアが実行され フル スイッチオーバー（SSO）モードで実行できるようになります。 この機能は、ソフトウェア アップグレード中に予定されたシステム停止中も同じレベル SSO を使用できます。つまり、システムをセカンダリ RP に切り替えることができ、セ がら、継続してパケットを転送できます。 この機能は、デフォルトでイネーブルにされています。 この機能により、新規追加または変更されたコマンドはありません。
SSO：GLBP		GLBP が SSO を認識するようになりました。GLBP は、ルータがセカンダリ RP にフェ することができます。 別の RP がインストールされ、プライマリ RP が機能を停止した場合にはその処理を引き これを認識できません。プライマリが機能を停止すると、GLBP デバイスは GLBP グル 内の他のルータにアクティブ ルータとしてのロールが引き継がれます。このように機能 出できるようになったため、GLBP グループに何ら変化は生じません。セカンダリ RP 態であると、GLBP グループはこの状態を検出して新たなアクティブ GLBP ルータを再 この機能は、デフォルトでイネーブルにされています。 **debugglbpevents**、**glbpsso**、**showglbp** の各コマンドがこの機能によって導入または修正

用語集

アクティブ RP：ルート プロセッサ（RP）はシステムの制御、ネットワーク サービスの提供、ルーティング プロトコルの実行、システム管理インターフェイスの有効化を実行します。

AVF：Active Virtual Forwarder（アクティブ仮想フォワーダ）。GLBP グループ内の 1 つの仮想フォワーダが、指定の仮想 MAC アドレスのアクティブ仮想フォワーダとして選定されます。選定されたフォワーダは、指定の MAC アドレスに対するパケットの転送を処理します。1 つの GLBP グループに複数のアクティブ仮想フォワーダを存在させることができます。

AVG：Active Virtual Gateway（アクティブ仮想ゲートウェイ）。アクティブ バーチャル ゲートウェイとして選択され、プロトコルの動作を担当する、GLBP グループ内の 1 つのバーチャル ゲートウェイ。

GLBP ゲートウェイ：Gateway Load Balancing Protocol ゲートウェイ。GLBP を実行するルータまたはゲートウェイ。各 GLBP ゲートウェイは、1 つまたは複数の GLBP グループに参加できます。

GLBP グループ：Gateway Load Balancing Protocol グループ。接続されたイーサネットインターフェイス上で同じ GLBP グループ番号を持つ、1 つまたは複数の GLBP ゲートウェイ。

ISSU：In Service Software Upgrade（インサービス ソフトウェア アップグレード）。パケット転送の実行中に Cisco IOS XE ソフトウェアの更新や変更を可能にするプロセス。ほとんどのネットワークでは、計画的なソフトウェアアップグレードがダウンタイムの大きな原因になっています。ISSU を使用すると、パケット転送中にソフトウェアを変更できるため、ネットワークのアベイラビリティが向上し、計画的なソフトウェアアップグレードによるダウンタイムを短縮できます。

NSF：Nonstop Forwarding（ノンストップ フォワーディング）。機能停止状態からの回復処理を行っているルータに対してトラフィックの転送を継続するルータの機能。また、障害からの回復中であるルータは、自身に送信されたトラフィックをピアによって正しく転送することができます。

RP：ルート プロセッサ。シャーシに搭載される、集中化されたコントロール ユニットの総称です。一般に、プラットフォーム固有の用語が使用されます（Cisco 7500 では RSP、Cisco 10000 では PRE、Cisco 7600 では SUP+MSFC など）。

RPR：Route Processor Redundancy。RPR は、High System Availability（HSA）機能に代替方法を提供します。HSA を使用すると、システムはアクティブ RP が機能を停止したときにスタンバイ RP をリセットして使用できます。RPR を活用すると、アクティブ RP に致命的なエラーが発生したときにアクティブ RP とスタンバイ RP の間で迅速なスイッチオーバーが行われるため、不測のダウンタイムを減らすことができます。

RPR+：RPR の拡張。スタンバイ RP が完全に初期化されます。

SSO：Stateful Switchover（ステートフル スイッチオーバー）。アクティブ装置とスタンバイ装置間のステート情報を保持するためのアプリケーションおよび機能をイネーブルにします。

スタンバイ RP：完全に初期化され、アクティブ RP から制御を引き受ける準備が整った RP。手動または機能停止によってスイッチオーバーが発生します。

スイッチオーバー：システム制御とルーティング プロトコルの実行がアクティブ RP からスタンバイ RP に移行するイベント。スイッチオーバーは、手動操作によって、またはハードウェア/ソフトウェアの機能停止によって発生します。スイッチオーバーには、個々のユニットのシステム制御とパケット転送を組み合わせるシステムでのパケット転送機能の移行が含まれることがあります。

vIP：仮想 IP アドレス。IPv4 アドレス。設定された各 GLBP グループには、必ず 1 つの仮想 IP アドレスがあります。仮想 IP アドレスは、少なくとも 1 つの GLBP グループ メンバに設定する必要があります。他の GLBP グループ メンバは、Hello メッセージを通して仮想 IP アドレスを学習します。